Kansas Information Technology Executive Council (ITEC)
ITEC Policy # 5200 Public Key Infrastructure Certificate Policy

ATTACHMENT 1

Certificate Policy

for the

State of Kansas

Public Key Infrastructure

Version 2.0
August 19, 2005

Table of contents

6 Technical security controls

7 Certificate and CRL profiles

8 Policy administration

APPENDICES

1 Agreement between RA and LRA
2 Agreement between LRA and Partner Subscriber
3 Individual Subscriber Agreement

1 Introduction

1.1 Overview

1.1.1 Policy overview

This certificate policy (CP) is adopted by the information technology executive council (ITEC), and it governs the issuance and use of certificates among those persons and devices authorized to participate in the public key infrastructure (PKI) described by this CP.

It supports digital signatures, encryption and access control applications in the following electronic environments:

- communications and transactions within, between and/or among agencies, departments, units and/or organizations which are a part of any governmental body (government agencies);

- communications and transactions among or between government agencies and other persons, as defined by Kansas law. Under the Kansas uniform electronic transactions act "person" means an individual, corporation, business trust, estate trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation or any other legal or commercial entity. Communications among persons regarding the following are covered:

  government;
  health care;
  health plans; and
  other subjects in the health care sector;
  universities;
  colleges;
  teaching and research;
  students and others in the academic sector;
  consumer activities; and
  any other purpose not specified above.

In particular, this policy describes the relationships within the PKI, among and between:

- persons in their capacity as subscribers to certificates;

- persons in their capacity as parties relying upon certificates issued under this policy (relying parties);

- a certification authority (CA) under this policy;

- persons acting as repositories under this policy;

- persons acting in the capacity of registration authorities (RA) and local registration authorities (LRA) under this CP; and

- the State of Kansas.

PKI and the Kansas Consolidated IT Governance Structure are organized as follows:

The Kansas IT governance structure, established in 1998 (KSA-75 7201 *et seq.*), unifies and consolidates the IT community in Kansas government. The governance model is designed so that each part of the community is made stronger by the presence of the other components.

ITAB The information technology advisory board (ITAB) is the foundation of the consolidated IT community model. The operational philosophy is both bottom-up and top-down with communication among the participants vertically and horizontally. The ITAB and sub-committees form the nucleus where many IT initiatives and projects are identified. The need for certain IT policies have genesis in ITAB as well. ITAB membership comes from state agency IT directors, regents' university IT directors (regents computer advisory council-RCAC), leadership of the information network of Kansas (INK), the state historical society and associate members including, technologists, functional users, subject matter experts and others in the IT field.

ITEC As set forth in KSA 75-7201 *et seq.* the information technology executive council (ITEC) is comprised of seventeen members from both state and local government and the private sector. Private sector membership is by gubernatorial appointment. The secretary of administration in the executive branch chairs ITEC. ITEC is charged with:

- IT policies, procedures and data management standards for the enterprise
- project management methodologies and project manager certification
- enterprise information technology architecture
- strategic information technology management plans for state agencies.

The ITEC is the owner of policy relating to critical technology implementation in Kansas.

ITIMG The information technology identity management group (ITIMG) reports to ITEC and is authorized by the ITEC to make day-to-day administrative and fiscal decisions for the PKI program. Its membership includes the executive, legislative and judicial chief information technology officers (CITOs), a representative of the INK, the secretary of state (secretary) or the secretary's designee and two agency CIOs designated by the secretary. The secretary is the chair of the ITIMG.

CITA The state chief information technology architect (CITA) reports to ITEC and is secretary of ITEC. The CITA is responsible for the Kansas information technology architecture (KITA), strategic information management (SIM) plan, IT project management standards, and IT policy development. The CITA will aid in the management and maintenance of the PKI certificate policy.

KITO The Kansas information technology office (KITO) supports ITEC and the CITA in day-to-day activities by preparing reports, plans, and policies and performing tasks necessary to conduct council business. Additionally, the KITO provides support to the CITOs in their role of project oversight, agency three-year IT plans and project management training. The KITO will provide support for the implementation of the PKI certificate policy.

CITO The Kansas IT governance structure provides for a chief information technology officer (CITO) for each of the three branches of Kansas government. The executive branch CITO reports to the governor. The judicial branch CITO reports to office of judicial administrator and then the supreme court. The legislative CITO reports to the joint legislative committee on information technology (JCIT) and then to the legislative coordinating council (LCC), comprised of members from the legislature. Each CITO fills the implementation role in the model within their respective branch and has significant input in policy direction. The CITOs are responsible for implementation of the PKI Certificate Policy and related activities within their respective branches of government.

Certificates issued under this policy may be used:

- to verify digital signatures;
- to encrypt and authenticate electronic communications; and
- to provide evidence of identity in order to support access controls.

1.1.2 Overview of transactions

The PKI governed by this policy makes use of CAs registered under the laws of the state of Kansas. Subscribers and relying parties not located in the State of Kansas may obtain and/or rely upon certificates issued under this policy, and such certificates may be used for transactions, applications and communications outside the State of Kansas, provided that the laws of the State of Kansas are applied as a matter of law, unless prohibited by federal law.

1.1.2.1 State registration of CAs

CAs under this policy shall be registered by the secretary in accordance with the Kansas uniform electronic transaction act (KUETA). KSA 16-1601 *et seq.*

1.1.2.2 Identity assurance and certificate types

This policy provides for four (4) types of certificates. One factor that differentiates each type is the degree of assurance relating to the subscriber's identity that is provided by (i) the procedures used to identify and authenticate (I&A) the subscriber prior to issuance of the certificate and (ii) the degree of security a subscriber is required to use to protect his/her private key under this policy. The four certificate types are designated levels one, two, three and four.

Security and convenience considerations must be balanced in selecting procedures for access to and the use of electronic systems, because any increase in security may cause a decrease in convenience. This PKI uses four certificate types in order to permit subscribers and relying parties to select the preferred balance between security and convenience for their intended uses.

The certificate type to be used for any given application, transaction or communication shall be determined by the parties using or engaging in that application, transaction or communication, based upon their judgment as to the appropriate balance between security and convenience for their purposes.

The I&A procedures and subscriber security obligations applicable to each certificate type are described below. Certificates may be issued to persons and electronic devices, subject to the limitations of this policy.

Certificates shall be issued under this policy following I&A of a subscriber's identity in the manner set forth in this policy. A CA shall revoke certificates in the circumstances enumerated in section 4.9. A CA shall maintain records and information logs in the manner described in sections 5.4 and 5.5.

		Private keys shall be created, used and stored in a trustworthy and secure manner. Keys shall have a validity period as indicated in this policy. Private keys issued by a CA shall be backed-up to protect against data loss or data corruption. A CA shall not disclose an applicant's or a subscriber's personal information except as provided in this policy. CA activities shall be subject to inspection and/or audit for compliance with this policy in accordance with section 2.7.
1.1.3	General definitions	Terms used herein and in related agreements and other documents incorporating this policy have the following meanings:
	Activation data	Private data, but not keys, used or required to access or activate cryptographic modules.
	Affiliated person	An individual person who is authorized by an organization to hold a certificate containing the organization's name as an employee, partner, member, officer, agent, licensee, permitee or other associate of the organization.
	Applicant	A subscriber, after applying to a CA for a certificate, but before the certificate is issued.
	Authenticate	To confirm the identity of a person when the person's identity information is presented.
	Authority revocation list (ARL)	A list of revoked CA certificates. An ARL is a CRL for CA cross-certificates.
	CA certificate	The certificate at the beginning of a certification chain within the State of Kansas PKI hierarchy, which is self-issued in a secure and trustworthy manner.
	CA private root key	The private key used to sign the CA certificate and certify the CA's public/private key pair.
	CA private signing key	The private key that corresponds to a CA's public key and is listed in the CA certificate and which is used to sign certificates.
	Certificate	A computer-based record or electronic message that at a minimum: (i) identifies the CA issuing it; (ii) names or identifies a subscriber; (iii) contains the public key of the subscriber; (iv) identifies the certificate's operations period; and (v) is digitally signed by a CA.
	Certificate policy (CP)	This policy, which states a named set of rules that indicate the applicability of a certificate to particular communities and classes of applications with common security requirements.
	Certificate profile	The protocol stated in section 7 of this policy, which establishes the allowed format and contents of data fields within a certificate.
	Certificate revocation list (CRL)	A list maintained by a CA of the certificates it has issued that are revoked before their stated expiration dates.
	Certification authority (CA)	A person providing certification of a digital signature who is, or is certified by, a member of the group of certification authorities approved by and registered with the secretary of state.

Certification practice statement (CPS)	A statement published by a CA that specifies the policies or practices that the CA employs in issuing, publishing, suspending and revoking certificates in compliance with this CP.
Chief information technology architect (CITA)	The Kansas chief information technology architect, acting in accordance with KSA 75-7204.
Chief information technology officer (CITO)	The Kansas chief information technology officer, one each for the three branches of Kansas government, acting in accordance with KSA 75-7205, 7206 and 7207.
Compliance review	Documentation in the form of an information systems audit report verifying the applicant has the use of a trustworthy system, as defined in Kansas law.
Cross-certificate	A certificate used to establish a trust relationship between two CAs.
Cryptomodule	Hardware and/or software that: (i) generates key pairs, (ii) stores cryptographic material and/or (iii) performs cryptographic functions.
Digital signature	A type of electronic signature consisting of a transformation of an electronic message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether: (i) The transformation was created using the private key that corresponds to the signer's public key; and (ii) the initial message has not been altered since the transformation was made.
Distinguished name (DN)	The unique identifier for a subscriber so that the person or device can be located in a directory.
Electronic device	Computer software or hardware or other electronic or automated means configured and enabled by the subscriber to act as its agent and to initiate or respond to electronic records or actions, in whole or in part, without review or intervention by the subscriber.
Erase	To remove all the data stored on a magnetic storage medium. This procedure also is referred to as "degaussing."
Federal information processing standards (FIPS)	FIPS are a set of standards that describe document processing, provide standard algorithms for searching and provide other information processing standards for use within US government agencies.
Globally unique identifier (GUID)	Also called a universally unique identifier (UUID); the result of a process that yields a character string, containing combinations of numbers, letters and/or special characters and that is appended to the common name (CN) in individual or entity certificates. This CP makes no provision for the length of the character string beyond that required by best industry practice. The GUID may contain only those characters found in the following character set: **ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789[ ]-**
Hardware token	A physical object (*e.g.* smartcard or a USB token) that is authenticated to and grants access to a system. It may store a subscriber's private keys and certificates.

High-security zone	An area to which access is controlled through an entry point and limited to authorized, appropriately screened personnel and properly escorted visitors, accessible only from security zones and separated from security zones and operations zones by a perimeter.
Identification and authentication (I&A)	To ascertain and confirm through appropriate inquiry and investigation the identity of a subscriber or other person.
Information network of Kansas (INK)	The information network of Kansas, acting in accordance with KSA 74-9301 *et seq.* and approved by ITEC to perform the duties of RA pursuant to KAR 7-41-1 *et seq.,* this CP, related agreements and other documents.
Information technology advisory board (ITAB)	The Kansas information technology advisory board.
Information technology executive council (ITEC)	The Kansas information technology executive council, acting in accordance with KSA 75-7202 *et seq.*
Information technology identity management group (ITIMG)	The information technology identity management group, reporting to and authorized by the ITEC to provide the day-to-day administrative and fiscal decisions for the PKI program.
Issue certificates	The acts performed by a CA in creating a certificate, listing itself as "issuer," and notifying the RA or other certificate applicant of its contents and that the certificate is ready and available for acceptance.
Kansas information technology office (KITO)	The Kansas information technology office.
Kansas uniform electronic transactions act (KUETA)	KSA 16-1601 *et seq.*
Key escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer or other party in accordance with provisions set forth in the agreement.
Key generation	The trustworthy process of creating a public/private key pair.
Key pair	Two mathematically related keys having the properties that (i) one key can be used to encrypt a message that only can be decrypted using the other key and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Level one certificate	No identification and authentication is required for this certificate. An applicant may apply and receive a certificate by providing his or her name and e-mail address.

Level two certificate	A certificate issued based upon I&A procedures, which include the applicant's application through a network such as the internet, by correspondence or in person. An applicant shall provide appropriate proof of identity, which may be accomplished by use of a database or by attestation of a trusted individual in the same organization who has supervisory responsibility for the applicant.
Level three certificate	A certificate issued based upon I&A procedures, which includes personal appearance before the RA and the providing of at least one approved Kansas government-issued official picture identification credential or two non-Kansas government-issued official identification credentials at least one of which must be a picture identification.
Level four certificate	A certificate based upon I&A procedures, which includes the requirements of a level three certificate and may include biometric data. The private key shall exist in a hardware token.
Lightweight directory access protocol (LDAP)	A software protocol for enabling anyone to locate organizations, individuals and other resources such as files and devices in a network, whether on the public internet or on a corporate intranet.
Local registration authority (LRA)	An entity that, because of its relationship of trust with subscribers, has a contractual relationship with an RA to accept applications and conduct I&A for those subscribers. In the conduct of these responsibilities, an LRA acts in compliance with the law, the provisions of this CP and the related agreements contained in this policy pertaining to RA duties.
Online certificate status checking protocol (OCSP)	A protocol identified by RFC internet engineering task force's (IETF) request for comment) 2560 that enables an application to determine the status of an identified certificate by issuing a status request to an OCSP responder and suspending acceptance of the certificate in question until the responder has provided the application with a response.
Operations zone	An area where access is limited to personnel who work there and to properly escorted visitors. Operations zones are monitored at least periodically, based on a threat risk assessment and preferably should be entered from a reception zone.
Operative personnel	Operative personnel are individual persons who are agents or employees of an RA, an LRA or a CA.
Out of band	Communication between parties using a means or method that differs from the current method of communication.
Person	Under the KUETA, an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation or any other legal or commercial entity.
Policy management authority (PMA)	For this policy, the ITIMG.
Private key	The key of a public/private key pair kept secret by its holder, used to create digital signatures and to decrypt messages or files that were encrypted with the subscriber's corresponding public key.

Public key	The key of a public/private key pair that is used to verify a digital signature created with its corresponding private key, which can be made available publicly in a certificate, and which also can be used to encrypt messages or files that can be decrypted only with the intended recipient's corresponding private key.
Public key cryptography	A type of cryptography also known as asymmetric cryptography that uses a unique public/private key pair of mathematically related numbers.
Public key infrastructure (PKI)	The architecture, organization, techniques, practices and procedures that collectively support the implementation and operation of a certificate-based public key cryptography system.
Reception zone	The entry to a facility where the initial contact between the public and a CA or RA occurs, where services are provided, information is exchanged and access to restricted (operations, security and high-security) zones is controlled. To varying degrees, activity in a reception zone is monitored by the personnel who work there, by other personnel or by security staff. Access by the public may be limited to specific times of the day or for specific reasons. Entry beyond the reception zone is indicated by a recognizable perimeter such as a doorway or an arrangement of furniture and dividers in an open office environment.
Registration	The process of receiving or obtaining a request for a certificate from a subscriber and collecting and entering the information needed from that subscriber to include in and support I&A and issuance of a certificate.
Registration Authority (RA)	A person who has been authenticated by a CA, issued a registration authority certificate by the CA and approved by ITEC to process subscriber applications for certificates and to conduct I&A of subscribers in accordance with the law, this policy and the related agreements.
Relying party	A person who relies on a certificate issued under the terms of this policy.
Relying party agreement	An agreement between a CA and any person under which the person has agreed to be bound by all of the provisions of this policy and a CA's certification practice statement.
Repository	Also directory. An online system maintained by or on behalf of a CA for storing and retrieving certificates and other information relating to certificates and digital signatures.
Revocation or revoke a certificate	To prematurely end the operational period of a certificate, effective at a specific date and time.
Secretary	The Kansas secretary of state.
Security zone	An area to which access is limited to authorized personnel and to authorized and properly escorted visitors. Security zones preferably should be accessible from an operations zone through a specific entry point. A security zone is not required to be separated from an operations zone by a secure perimeter. A security zone is monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means.
Shared secret	Activation data used to assist parties in authenticating identity and establishing a

	reliable channel of communication.
Software cryptomodule	A software program that performs the functions of a cryptomodule.
Sponsoring organization	An organization that has authorized the issuance of a certificate identifying the subscriber as having an affiliation with the organization (*e.g.*, as an employee, partner, member, officer, agent, licensee, permitee or other associate).
State	The State of Kansas.
Strong PIN or password	An alphanumeric code of at least eight characters, consisting of a combination of upper case, lower case, special characters and numbers, used to gain access to a password-protected system.
Subscriber	A person who is the subject of a certificate, accepts the certificate and holds the private key that corresponds to the public key listed in that certificate.
Third party identity proofing	A process by which an RA confirms subscriber information provided during registration by verifying it with other organizations and agencies that serve as information or reference services.
Trusted role	A role whose incumbent performs functions that may introduce security problems if not carried out properly, whether accidentally or intentionally.
Trustworthy system	A secure system that materially satisfies the most recent common criteria protection profile for commercial security, known as "CSPP – guidance for COTS security protection profiles," published by the U.S. department of commerce in December 1999 and hereby adopted by reference. (The previous version of this document was known as "CS2 – protection profile guidance for near-term COTS.")

1.1.4 Acronyms

ANSI	American national standards institute
ARL	authority revocation list
CA	certification authority
CITA	chief information technology architect
CITO	chief information technology officer
CP	certificate policy, used interchangeably with " ITEC policy"
CPS	certification practice statement
CRL	certificate revocation list
DN	distinguished name
FIPS	federal information processing standards
I&A	identify or identification and authenticate or authentication

	IETF	internet engineering task force
	INK	information network of Kansas
	ITAB	information technology advisory board
	ITEC	information technology executive council
	ITIMG	information technology identity management group
	KAR	Kansas administrative regulations
	KITO	Kansas information technology office
	LDAP	lightweight directory access protocol
	LRA	local registration authority
	KSA	Kansas statutes annotated
	KUETA	Kansas uniform electronic transactions act
	OID	object identifier
	OCSP	online certificate status protocol
	PKI	public key infrastructure
	RA	registration authority
	PKIX	public key infrastructure X.509
	PMA	policy management authority
	SOS	secretary of state
	X.500	the ITU-T (international telecommunication union-T) standard that establishes a distributed, hierarchical directory protocol organized by country, region, organization, etc.
	X.509	the ITU-T standard for certificates. X.509, version 3, refers to certificates containing or capable of containing extensions.

1.2 Identification

1.2.1	OID requirement	If the state of Kansas secures an OID, it shall do so in compliance with the ANSI protocol.

1.3 Community and applicability

1.3.1	Open-but-bounded infrastructure	This policy describes an open-but-bounded (OBB) public key infrastructure, as described in the IETF public key infrastructure X.509 (PKIX) part 4 framework. A certificate issued in an OBB PKI may be relied upon by multiple parties. A CA in an OBB PKI is a legal entity independent of its subscribers and relying parties. A CP adopted for an OBB PKI reflects the agreements and understandings of the parties using the PKI. The OBB PKI described in this policy is based in the State of Kansas, and this policy shall be interpreted and enforced under the provisions of the Kansas uniform electronic transactions act and the Kansas administrative regulations. Certificates issued pursuant to this policy may be used for communications and transactions and by parties within or outside the State of Kansas, and between parties within and parties outside the State of Kansas. This policy describes the rights and obligations of persons authorized under this policy to fulfill any of the following roles: certificate service provider roles, end entity roles and policy management authority roles. Certificate service provider roles are CA, RA and repository. End entity roles are subscribers and relying parties. Requirements for persons authorized to fulfill any of these roles are in this section.
1.3.2	The policy management authority (PMA)	The PMA for this CP has delegated authority from ITEC and advises the ITEC on policy matters.
1.3.3	Registration authorities (RAs) and local registration authorities (LRAs)	Under this policy, RA functions are conducted by RAs approved by the ITEC or by LRAs who have executed an agreement with an RA to perform such functions in its stead. RAs and LRAs shall comply with the law and this CP, including the related agreements contained in this policy.
1.3.4	Repositories	A CA shall perform the role and functions of the repository. A CA may subcontract performance of the repository functions to a third party repository who agrees to be bound by all of the provisions of this policy, but a CA remains responsible for the performance and audit of those services in accordance with this policy.
1.3.5	End entities	Subscribers and relying parties are end entities for this CP.
1.3.5.1	Subscribers	A subscriber is the person whose name appears as the subject in a certificate and uses the certificate and corresponding keys in accordance with this policy. A CA may issue certificates that reference this policy to persons and electronic devices, provided that responsibility and accountability is attributable to an individual person as custodian of the public/private key pair.
1.3.5.2	Relying parties	A relying party is any person who relies upon a certificate issued under the terms of this policy.

1.3.6	Applicability and applications	Pursuant to this CP, the relying party determines whether to rely upon the certificate; the certificate may support signature, encryption, authentication and/or access; prohibited use is defined; and cross-certification may be approved.
1.3.6.1	Determination of acceptability of certificate type by relying party	This policy does not specify what steps the relying party should take to determine whether to rely upon the certificate. For example, it does not compel the relying party to perform X509 path creation or processing or to determine whether any certificates in the trust path have been revoked. The relying party decides, pursuant to its own or its agency's/organization's policies, what steps to take; the policy merely provides the tools needed to perform the trust path creation, validation and certificate policy mappings that the relying party may wish to employ in its determination. In addition, except for the provisions of 1.3.6.3, this policy contains no limits on the use of any certificates, issued by the CA or by RAs. Instead, persons acting as relying parties shall determine what financial or liability limits, if any, they wish to impose for certificates used to consummate a transaction.
1.3.6.2	Purposes	Certificates that reference this policy are intended to support verification of digital signatures in applications where the identity of communicating parties needs to be authenticated, where a message or file needs to be bound to the identity of its originator by a signature, where the integrity of the file or message has to be assured to enable encryption for confidential communications and for authentication and for access control. The suitability of a given certificate for any given purpose depends upon the level of assurance of the identity of the subscriber required by a relying party for that purpose and the acceptability of digital signatures under applicable law.
1.3.6.3	Prohibited applications	If certificates that reference this policy are proposed to be used by any authority having jurisdiction over an application requiring fail safe performance (such as the operation of nuclear power facilities, air traffic control systems, aircraft navigation systems, weapons control systems or any other system whose failure could lead to injury, death or material environmental damage), the authority having jurisdiction over such application and who proposes such use first shall obtain approval for use of the certificates from the ITEC.
1.3.6.4	Cross-certification	The PMA may approve the issuance of a cross-certificate between CAs. Any such cross-certification only shall occur after approval by the PMA and notice to the secretary and all RAs.

1.4 Contact details

1.4.1	Specification/policy administration organization	Communication to the PMA should be addressed to: ITIMG Secretary of State First Floor, Memorial Hall 120 SW 10th Av Topeka, KS 66612-1594
1.4.2	Contact person	Questions regarding the implementation and administration of this policy should be directed to: Assistant Secretary of State First Floor, Memorial Hall 120 SW 10th Av Topeka, KS 66612-1594

1.4.3	Person determining CPS suitability for policy	The PMA shall determine the suitability of any CPS to this policy.

2 General provisions

2.1 Apportioning legal responsibilities among parties

2.1.1 CA obligations, representations and liability

A CA shall conduct the following aspects of the issuance and management of certificates:

- acceptance of completed applications and enrollment materials for certificates from RAs and enrollment of subscribers upon such acceptance;
- the certificate manufacturing process;
- publication, suspension, revocation and renewal of certificates;
- administration of the repository; and
- management of CA operations and infrastructure related to certificates in accordance with the requirements, representations and warranties of this policy.

2.1.1.1 Notification of certificate issuance and revocation

A CA shall make CRLs available to subscribers and relying parties in accordance with section 4.9. A CA shall notify an RA or, when appropriate, a subscriber when a certificate bearing the subscriber's DN is issued or revoked.

2.1.1.2 Accuracy of representations

By issuing a certificate that references this policy, a CA certifies and warrants to the subscriber and to all parties who reasonably rely on the information contained in the certificate during its operational period and in accordance with this policy that:

- the CA has issued and will manage the certificate in accordance with this policy;
- the CA has complied with the requirements of this policy and any applicable CPS when authenticating the subscriber and issuing the certificate;
- there are no misrepresentations of fact in the certificate reasonably known to the CA, and the CA has taken reasonable steps to verify any additional information in the certificate;
- information provided to the CA by the RA and/or subscriber in the certificate application for inclusion in the certificate has been transcribed accurately to the certificate; and
- the certificate meets all material requirements of this policy and the CA's CPS.

2.1.1.3 Time between certificate request and issuance

After completion of I&A, certificates shall be issued within three (3) business days.

2.1.1.4	Certificate revocation and renewal	A CA shall ensure that any procedures for the expiration, revocation and renewal of a certificate will conform to the relevant provisions of this policy and will be expressly stated in the subscriber agreement and any other applicable document outlining the terms and conditions of the certificate use. A CA shall ensure that key changeover procedures are in accordance with section 5.6. A CA also shall ensure that notice of revocation of a certificate will be posted to the CRL within the time limits stated in section 4.9. The address of the CRL shall be defined in the certificate.
2.1.1.5	Protection of private keys	A CA shall ensure that its private keys and activation data are protected in accordance with parts 4 and 6 of this policy.
2.1.1.6	Restrictions on CA's private key use	A CA shall ensure that its CA private signing key is used only to sign certificates and CRLs. A CA may issue certificates to subscribers, CA and RA personnel, devices and applications. A CA shall ensure that private keys issued to its personnel, employees, officers, agents and subcontractors to access and operate CA applications are used only for such purposes.
2.1.1.7	Ensure compliance	A CA shall ensure that *only it* accepts and uses registration information transmitted as follows: (i) directly to the CA from subscribers or (ii) directly from an RA. A CA shall ensure that its certification and repository services, issuance and revocation of certificates and issuance of CRLs are in accordance with this policy. The CA shall ensure that its authentication and validation procedures are implemented as set forth in part 3.
2.1.1.8	Consequences of breach	Reserved.
2.1.1.9	Notification of breach	The CA shall advise the secretary and the PMA at the earliest possible time of any breach or suspected breach.
2.1.1.10	Conflict	Nothing in this policy shall be construed to conflict with, alter or eliminate any other obligation, responsibility or liability that may be imposed on any person by virtue of any contract or obligation that is otherwise determined to be controlling by applicable law.
2.1.2	RA and LRA obligations, representations	Each RA and LRA with whom it has executed an agreement for RA services shall comply with the law, this CP and the related agreements contained in this policy when providing registration, authentication and other RA services.
2.1.3	Subscriber obligations, representations and liability	The responsibilities of each subscriber for a certificate shall be:
2.1.3.1	Representations	Upon application for a certificate and in all subsequent communications, to provide complete and accurate responses to all appropriate requests for information made by the CA or RA during the applicant registration, certificate application and authentication of identity processes; and, upon notice to the subscriber of issuance of a certificate naming the applicant as the subscriber, to review the certificate to ensure that all subscriber information included in it is accurate and to accept or reject the certificate in accordance with section 4.4;
2.1.3.2	Subscriber security obligations/	To generate a key pair using a secure system, and to take appropriate precautions to prevent any compromise, modification, loss, disclosure or unauthorized use of the

	protection of subscriber private key and hardware token	private key. "Appropriate precautions" and "secure system," for purposes of the different types of certificate provided for in this policy, shall mean the following:
2.1.3.2.1	Level one and level two certificates	To use reasonable efforts to protect the private key for level one and level two certificates, which may be stored in the browser of any computer at the subscriber's election and risk. Use of a password or PIN to protect the private key shall be required.
2.1.3.2.2	Level three and level four certificates	To use reasonable efforts to protect the private key for a level three and level four certificates, which shall include storage in a hardware token or software cryptomodule protected by a strong PIN or password.
2.1.3.3	Restrictions on end-entity private key use	To use the certificate and the corresponding private key only for purposes authorized by and consistent with the law, this CP and the related agreements; and
2.1.3.4	Notification upon private key compromise	To instruct the CA or RA to revoke the certificate promptly upon any actual or suspected loss, disclosure or other compromise of the private key, or, in the case of a certificate issued to an affiliated individual, when the affiliated individual no longer is affiliated with the organization.
2.1.3.5	Consequences of breach	A subscriber who is found to have acted in a manner inconsistent with these obligations shall have his or her certificate revoked and shall forfeit all claims he or she may have against any other party to the PKI in the event of a dispute arising from the failure to fulfill the obligations above.
2.1.4	Relying party obligations, representations and liability	Before using a subscriber's certificate, a relying party shall ensure that it is appropriate for the intended use.
2.1.4.1	Revocation check responsibility	A relying party shall check the status of the certificate through OCSP or against the appropriate and current CRL in accordance with the requirements stated in section 4.9 (as part of this verification process the digital signature of the CRL also shall be validated).
2.2	***Limitation on liability***	Reserved.
2.3	***Financial responsibility***	
2.3.1	A CA	A CA shall obtain and maintain a good and sufficient surety bond, certificate of insurance or other evidence of financial security in the amount of $100,000. Pursuant to Kansas law, if the CA fails to comply with this provision, the CA's registration with the secretary may be deemed lapsed.
2.4	***Interpretation and enforcement***	
2.4.1	Governing law	The laws of the United States of America and the State of Kansas shall govern the enforceability, construction, interpretation and validity of this policy.

2.4.2	Specific provisions: merger and notice	A CA shall ensure that any agreements by that CA will contain provisions governing severability, survival, merger or notice consistent with Kansas law.
2.4.3	Dispute resolution procedures	ITEC, with assistance from the PMA, shall resolve any disputes associated with the use of the CA or certificates issued by the CA.
2.5	***Fees***	Reserved
2.6	***Publication and repository***	
2.6.1	Publication of CA information	A CA shall operate a secure on-line repository that is available to relying parties and that contains (i) issued certificates that reference this policy, (ii) a certificate revocation list (CRL) or on-line certificate status database, (iii) the CA's certificate for its CA private signing key, (iv) past and current versions of the CA's CPS, (v) a copy of this policy and (vi) other relevant information relating to certificates that reference this policy.
2.6.2	Frequency of publication	Certificates shall be published following the subscriber acceptance procedure specified in section 4.4. The CRL shall be published as specified in section 4.9.
2.6.3	Access controls	A CA shall not impose any access controls on this policy, the CA's certificate for its CA private signing key and past and current versions of the CA's CPS. A CA may impose access controls on certificates and certificate status information in accordance with provisions of this policy.
2.6.4	Location	The location of publication shall be one that is convenient to the certificate-using community and appropriate to the total security requirements. It shall identify an X.500 directory and an LDAP interface.
2.6.5	Revocation information	The sole sources of information regarding the validity or revocation of a certificate shall be provided by an RA, the CA or a repository.
2.7	***Compliance reviews***	
2.7.1	Frequency	A CA shall submit to and pay for compliance reviews applicable to registered certification authorities under Kansas law. An applicant CA and a CA shall file the review report with the secretary upon initial registration as a CA and thereafter once every two years unless ordered as follows. The secretary or the PMA may order a compliance review at any time at their discretion.
2.7.2	Identity and qualifications of auditor	A compliance auditor shall be qualified to conduct a compliance review pursuant to Kansas law and shall be sufficiently familiar with the best practices of a CA.
2.7.3	Auditor's neutrality	The auditor(s) and CA shall have a contractual relationship for the performance of the review, and the auditor(s) shall be sufficiently separated legally and organizationally from the CA to provide an arms-length, unbiased, independent evaluation.

2.7.4	Scope of reviews	Reviews shall be conducted in accordance with Kansas law and in accordance with the most current version of "CSPP – guidance for COTS security protection profiles," published by the U.S. department of commerce.
2.7.5	Communication of results	The results of any reviews of the CA shall be reported to the CA and filed with the PMA and with the secretary as required by Kansas law.
2.7.6	Actions taken as a result of review	If a review reports any material noncompliance with applicable law, this policy or any other contractual obligations of a CA, the registration of the CA may be deemed lapsed in accordance with Kansas law.

2.8 Privacy and data protection policy

2.8.1	Use of subscriber information	A CA shall use subscriber information only for the purpose of performing the authentication process and issuing a certificate.
2.8.2	Private key information	Digital signature private keys shall be confidential. Any private key management keys held by a CA shall be confidential. Never shall any private key appear unencrypted outside the cryptographic module.
2.8.3	CA information	All information stored locally on CA equipment shall be secured as confidential information, and access to it shall be restricted to those with an official need-to-know in order to perform their official duties with regard to the PKI. Private keys used to sign certificates that will assert security privileges shall be classified at the same level as the privileges that are to be asserted by the related certificates. If a CA does not independently verify security privilege information, this requirement shall be executed by the RAs.
2.8.4	Compliance review information	Compliance review information is confidential and shall not be disclosed to anyone for any purpose except for conduct of the compliance review, reporting obligations pursuant to this policy, the CA contract with the secretary, the Kansas UETA and the KARs.
2.8.5	Permitted acquisition of private information; disclosure	A CA only shall collect such personal information about a subscriber that is required for the issuance of a certificate to the subscriber. For the purpose of proper administration of certificates, a CA or RA may request non-certificate information to be used in issuing and managing certificates (*e.g.*, identifying numbers, business or home addresses and telephone numbers). Collection of personal information shall be subject to collection, maintenance, retention and protection requirements of applicable state and federal law.
2.8.6	Opportunity of owner to correct private information	Information shall be made available by a CA or RA to the subscriber involved, following an appropriate written request by such subscriber, and shall be subject to correction and/or revision by the subscriber.
2.8.7	Release of information for criminal or civil matter, PMA and secretary roles	Only the PMA or secretary may authorize disclosure of certificate or certificate-related information to a law enforcement agency or other duly-authorized agent in a criminal or civil matter and only under the following circumstances: when (i) required to be disclosed by law, governmental rule or regulation or court order; or (ii) authorized by the subscriber when necessary to effect an appropriate use of the certificate. Any request for such disclosure of private and/or confidential information shall be made in accordance with applicable law.

2.9 Intellectual property rights

2.9.1	Private key ownership	The private key shall be treated as the sole property of the legitimate holder of the corresponding public key identified in a certificate. This certificate policy and its OID are the property of the ITEC and may be used by an RA or a CA in accordance with the provisions of this policy. Any other use of the above without the express written permission of the ITEC through the PMA is prohibited.

2.10 Validity of certificates

2.10.1	Acceptance	The act of accepting a certificate by a subscriber shall be logged by the CA and may consist of a record made when the certificate subject downloads the certificate. Such act shall be recorded and maintained in an auditable trail kept by the RA or CA in a trustworthy manner that complies with industry standards and any applicable laws.
2.10.2	Operational period	Unless accepted or waived by a relying party, after its expiration date an expired certificate no longer shall be used for purposes of authentication, signing and non-repudiation.
2.10.3	Validity of actions during operational period and legal	All relying parties' digital signature verification applications shall be capable of verifying that the digital signature was created during the certificate's operational period.

3 Identification and authentication

3.1 Duties of identification and authentication

3.1.1	Trustworthy procedures	The PMA shall establish trustworthy procedures whereby RAs may be authenticated by the CA and issued a certificate.
3.1.2	Rules for interpreting various name forms	A CA shall defer to a naming authority for guidance on name interpretation and subordination.
3.1.3	Uniqueness of names	The subject name listed in a certificate shall be unambiguous and unique for all certificates issued by a CA and shall conform to X.500 standards for name uniqueness. Additional numbers or letters shall be appended to the real name (to ensure the name's uniqueness within the domain of certificates issued by a CA) and shall conform to the definition of the GUID stated in this policy. Each name shall be unique and dedicated to a single unique entity.
3.1.4	Name claim dispute resolution procedure	Although a CA shall defer to a naming authority, as described in 3.1.2, it ultimately shall exercise sole discretion in determining subscriber names for certificates it issues. If necessary, a party requesting a certificate may be required to demonstrate its right to use a particular name. The CA shall investigate, and correct if necessary, any name collisions brought to its attention. A name collision shall be deemed a compromise of the CA's security and shall be remedied in accordance with its CPS and

this policy.

3.1.5	Method to prove possession of private key	Subscribers shall prove possession of the private key corresponding to the public key in a certificate request. For signature keys, this may be accomplished by signing the request. Before the issuance of a certificate, the subscriber shall confirm its identity using an appropriate secure protocol selected by the CA in consultation with the PMA. For encryption keys, a CA may encrypt the subscriber's certificate in a confirmation request message. The subscriber then may decrypt and return the certificate to the CA in a confirmation message. Other procedures also may be acceptable. If the private key is generated directly on a hardware token or smart card, or in a key generator that benignly transfers the key to the token or smart card, then the subscriber is deemed to be in possession of the private key at the time of generation or transfer. If the subscriber is not in possession of the token or smart card when the key is generated, then the token or smart card shall be delivered immediately to the subscriber by a trustworthy and accountable method (see section 6.1.2).

4 Certificate life cycle operations requirements

4.1 Certificate request

4.1.1	Required information and procedures	This policy identifies the required information and procedures that constitute assurance and support trust in the PKI. The following procedures satisfy the security requirements of this document. The following steps shall be required when applying for a certificate: establish the identity of subject; obtain a public/private key pair for each certificate required; prove to the CA that the public key forms a functioning key pair with the private key held by the user; provide a point of contact for verification of any roles or authorizations requested.
4.1.2	Who can request a certificate	An applicant for a certificate shall complete a certificate application in a form prescribed by the RA or CA and enter into a subscriber agreement with the RA and CA. All applications shall be subject to review, approval and acceptance by the RA and CA.
4.1.3	Certificate request process	An applicant for a certificate shall complete a certificate application and provide requested information in a form prescribed by the RA or CA and this policy.
4.1.4	Time to process a certificate request	Reserved.
4.1.5	Application for cross-certificate	The PMA, in consultation with a CA, shall specify procedures to apply for a cross-certificate.

4.2	***Certificate application validation***	Reserved.
4.3	***Certificate issuance***	
4.3.1	Applicant notification	Upon successful completion of the subscriber I&A process and complete and final approval of the certificate application, the CA shall issue the requested certificate, notify the RA and applicant thereof and make the certificate available to the applicant pursuant to a procedure whereby the certificate is initially delivered to, or available for pickup by, the subscriber only. The CA shall not issue a certificate without the consent of the applicant and, if applicable, the applicant's sponsor.
4.3.2	Issuance by CA, exception	Except for level one certificates, a CA shall use an out-of-band notification process linked to the certificate applicant's physical U.S. postal mail address, or equivalent, and deliver the certificate only to the subscriber.
4.3.3	Notification of certificate issuance to subscribers	After successful validation of the certificate application and issuance of the certificate, the CA shall notify the RA and subscriber in a trustworthy and confidential manner that the certificate has been issued.
4.4	***Certificate acceptance***	
4.4.1	Certificate acceptance	Acceptance is the action by a subscriber that triggers the subscriber's duties and potential liability and that constitutes acceptance of this CP, the related agreements and the CA's CPS. The CA shall define in its CPS a technical or procedural mechanism to explain the subscriber responsibilities defined in section 2.1.3, inform the subscriber of the creation of a certificate and the contents of the certificate and require the subscriber to indicate acceptance of the responsibilities and the certificate. This process will depend on factors such as where the key is generated and how certificates are posted, *e.g.* a subscriber may agree to its responsibilities at the same time that it accepts the certificate, or agreeing to its responsibilities may be a precondition for requesting a certificate.
4.4.2	Certificate acceptance by the subscriber	As a condition to issuance of the certificate, the subscriber shall submit acceptance or rejection of the certificate to the registered RA or LRA and complete the subscriber agreement contained in this policy. By accepting the certificate, the subscriber warrants that all information and representations made by the subscriber, which are included in the certificate, are true.
4.4.3	Notification of certificate issuance to others	Notification of certificate issuance to others may be accomplished by publication of the certificate in a recognized repository.

4.5 Certificate use

4.5.1	RA and CA responsibility	The RA and CA assume no responsibility for the use of or reliance upon certificates except as provided under this policy.

4.6 Routine certificate renewal

4.6.1	Automatic renewal	Routine certificate renewal may be performed by automatic renewal or recertification and shall create a new key pair.

4.7 Processing a request for a new key

4.7.1	Circumstances for request of a new key certification	If out-of-band processes (*e.g.* a shared secret) remain in place to authenticate the subscriber requesting new key certification, the RA and CA are not required to re-perform I&A of the subscriber.
4.7.2	Who can request certification of a new key	Only the RA or subscriber may request certification of a new key.
4.7.3	Treatment of a request for certification of a new key	Complete re-authentication of a subscriber is not required if out-of-band processes remain in place to authenticate the requester, including, for example, the use of a shared secret or bio-metric means of identity verification.
4.7.4	Notification of certification request for a new key to subscriber	The notification procedures used by the RA or CA shall be identical to procedures for a new subscriber request.

4.8 Certificate modifications

Reserved.

4.9 Certificate revocation

4.9.1	Circumstances for revocation, permissive revocation	An RA or subscriber may request revocation of a certificate at any time for any reason. A sponsoring organization may request revocation of an affiliated individual certificate at any time for any reason. A CA also may revoke a certificate upon failure of the subscriber or any sponsoring organization to meet its obligations under this policy, the applicable CPS, or any other agreement, regulation or law applicable to the certificate. This includes revoking a certificate when a suspected or known compromise of the private key has occurred. If the failure is that of an RA or sponsoring organization, the CA first shall notify the PMA of its proposed action.
4.9.2	Required revocation	An RA, subscriber, or a sponsoring organization promptly shall request revocation of a certificate: when the name on the certificate no longer is current, complete or true; when the private key, or the medium holding the private key, associated with

		the certificate is known to be or suspected to be lost, disclosed, compromised or subjected to unauthorized use in any way; or, when an affiliated individual no longer is affiliated with an RA or sponsoring organization. A CA shall revoke a certificate: upon request of the RA, subscriber or sponsoring organization; upon failure of the subscriber or the sponsoring organization to meet its material obligations under this policy, any applicable CPS, or any other agreement, regulation or law applicable to the certificate; if knowledge or reasonable suspicion of compromise is obtained; if the CA determines that the certificate was not properly issued in accordance with this policy and/or any applicable CPS. If the failure is that of an RA or sponsoring organization, the CA first shall notify the PMA of its proposed action.
4.9.3	Who can request revocation	A CA summarily may revoke certificates within its domain, provided that notice and cause are given. An RA may request the revocation of a subscriber's certificate on behalf of the subscriber, the subscriber's sponsoring organization or other authorized party. The subscriber is authorized to request the revocation of his or her own certificate, as is the subscriber's sponsoring organization.
4.9.4	Procedure for revocation request	A certificate revocation request shall be communicated promptly to the CA, either directly or through the RA authorized by ITEC to accept such notices. A certificate revocation request may be communicated electronically if it is digitally signed with the private key of the subscriber or the sponsoring organization. Alternatively, the subscriber or sponsoring organization may request revocation by contacting the RA or the CA in person and providing adequate proof of identification in accordance with this policy or an equivalent method.
4.9.4.1	Revocation request grace period	A CA shall revoke a certificate as quickly as practical upon receipt of a proper revocation request and always shall revoke certificates within the time periods described in this section 4.9. Notwithstanding the foregoing, there shall be a grace period of three (3) hours between the time a subscriber makes a revocation request and the time a certificate is revoked.
4.9.4.2	Suspension	A certificate may be suspended following an unsigned request for certificate revocation, pending authentication of the revocation request.
4.9.5	Time to process a revocation request	Promptly following revocation of a certificate, the CRL or certificate status database in the repository, as applicable, shall be updated. All revocation requests and the resulting actions taken by the CA shall be archived. Certificates may be revoked prior to their expiration. Revocation is accomplished by notation or inclusion in a set of revoked certificates or other directory or database of revoked certificates.
4.9.6	CRLs	CRLs shall be issued periodically as follows:
4.9.6.1	CRL issuance frequency	To ensure timeliness of information, CRLs shall be issued daily, even if there are no changes or updates to be made. CRLs may be issued more frequently than required; if there are circumstances for which the CA will post early updates, the circumstances shall be described with specificity in the CPS. The CA shall ensure that superceded CRLs are removed from the directory system upon posting of the latest CRL. If a CRL is issued as a result of a key compromise or revocation, the CRL shall be posted as quickly as feasible, but in any event shall be posted no later than six hours after notification of the compromise or decision to revoke by the CA. CAs shall make public the details of certificate revocation information posting, including an explanation of the consequences of using dated revocation information. This information shall be given to subscribers during certificate request or issuance and

		shall be readily available to relying parties.
4.9.6.2	CRL latency	Interim CRLs shall be made available to relying parties.
4.9.7	On-line revocation/status checking	When an on-line certificate status database is used as an alternative to a CRL, such database shall be updated and checked in accordance with the same requirements as defined for a CRL.
4.9.7.1	Online revocation/status checking availability	CAs shall validate online, near real time the status of the certificate identified in a certificate validation request message.
4.9.7.2	Online revocation checking requirements	Each relying party shall validate every certificate it receives in connection with a transaction in accordance with and by the means identified in the certificate. If it becomes infeasible to obtain revocation information, then the relying party either shall reject use of the certificate or make an informed decision to accept the risk, responsibility and consequences for using a certificate for which authenticity cannot be guaranteed to the standards of this policy.
4.9.7.3	Other forms of revocation notices available	A CA also may use other methods to publicize revoked certificates.

4.10 Certificate status services

4.10.1	Certificate status	See 4.9.6
4.10.2	End of subscription	If a person's subscription to the PKI ends prior to the expiration of any certificates issued under that subscription, the CA shall revoke any certificates issue or held under the subscription.
4.10.3	Private key recovery	A private signing key never shall be stored for purposes of recovery by a CA. If a key pair is used for both signature and confidentiality purposes, recovery of the private key is prohibited.

5 CA facility and management controls

5.1 Physical controls

5.1.1	Physical security controls	A CA and repositories shall implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations and any external cryptographic hardware modules or tokens) used in connection with providing CA services. Access to such hardware and software shall be limited to those personnel performing in a trusted role, as described in the section on procedural controls (5.2.1). Access shall be controlled through the use of electronic access controls, mechanical combination locksets or deadbolts. At all times, such access controls shall be monitored manually or electronically for unauthorized intrusion.

5.1.2 Site location and construction

Any CA site shall:

- satisfy the requirements for a security zone;
- be monitored manually or electronically for unauthorized intrusion at all times;
- ensure access to the CA server is limited to those personnel identified on an access list and implement dual access control requirements to the CA server for such personnel;
- ensure personnel not on the access list are properly escorted and supervised;
- ensure a site access log is maintained and inspected periodically; and
- ensure all removable media and paper containing sensitive plain text information are stored in containers either listed in or of equivalent strength as those listed in the security equipment guide.
- the location of the CA server shall satisfy the requirements for a high-security zone.

5.1.3 Physical access

CA equipment always shall be protected from unauthorized access. Removable CA cryptomodules shall be inactivated and placed in locked containers that will provide security commensurate with the classification, sensitivity or value of the information being protected by the certificates issued. Any activation information used to access or enable the cryptomodule or CA equipment shall be stored separately. Such information shall be memorized.

A security check covering the facility that houses CA equipment shall occur at least once every 24 hours. The check shall ensure that: the equipment's status is appropriate to the current mode of operation (*e.g.*, that cryptomodules and removable hard disks are in place when "open", and secured when "closed"); any security containers are properly secured; physical security systems (*e.g.*, door locks, vent covers) are functioning properly; and the area is secured against unauthorized access. A specifically identified position or person shall be responsible for making such checks. When a position is responsible, a log identifying the individual performing such a check shall be maintained. A record shall be kept that describes the types of checks performed, the time and the person who performed them. If the CA equipment is located in a continuously attended facility, there shall be a security check of the facility at least once per shift. If the facility is not continuously attended, the last person to leave the facility shall initial a sign-out sheet that states that the facility entrance door is locked and that, where installed, intrusion detection systems are activated. If the facility housing the CA equipment will be unattended for periods greater than 24 hours, it shall be protected by an intrusion detection system. Additionally, a check shall be made at least once every 24 hours to ensure that all doors to the facility are locked and that there have been no attempts by unauthorized persons to enter.

5.1.4 Power and air conditioning

The facility, which houses CA equipment, shall be supplied with power and air conditioning sufficient to create a reliable operating environment. In addition, personnel areas within the facility shall be supplied with sufficient utilities to satisfy operational, health and safety needs. The actual quantity and quality of utility service will depend on how the facility operates, *e.g.*, its times of operation (24

hours/7 days or 8 hours/5 days) and whether on-line certificate status checking is provided. The CA equipment shall have backup capability sufficient to automatically lockout input, finish any pending actions and record the state of the equipment before lack of power or air conditioning causes a shutdown. Users who require extended operation hours or short response times may contract with the CA for additional requirements for backup power generation. The revocation operations shall be supported by uninterruptible power supplies and sufficient backup power generation.

5.1.5 Water exposure

This policy makes no provision for prevention of exposure of CA equipment to water beyond that called for by best business practice. CA equipment shall be installed so that it is not in danger of exposure to water, *e.g.*, placement on tables or elevated floors. Moisture detectors shall be installed in areas susceptible to flooding. CA operators who have sprinklers for fire control shall have a contingency plan for recovery should the sprinklers malfunction or cause water damage outside of the fire area.

5.1.6 Fire prevention and protection

This policy makes no provision for prevention of exposure of CA equipment to fire beyond that called for by best business practice. An automatic fire extinguishing system shall be installed in accordance with local code. A CA shall have a contingency plan, which contemplates and addresses damage by fire.

5.1.7 Media storage

Media shall be stored in a manner that protects it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive or backup information shall be stored in a location separate from the CA equipment.

5.1.8 Waste disposal

Normal office waste shall be removed or destroyed in accordance with best business practices. Before disposal, media used to collect or transmit information discussed in section 2.8 shall be erased.

5.1.9 Off-site backup

System backups, sufficient to provide recovery from system failure, shall be made on a periodic schedule, which shall be described in the CPS. At least one backup copy shall be stored at an offsite location (separate from the CA equipment).
Only the latest backup is required to be retained. The backup shall be stored at a site with physical and procedural controls commensurate with that of the operational CA system.

5.2 Procedural controls

5.2.1 Trusted roles

A trusted role is one whose incumbent performs functions that may introduce security problems if not carried out properly, whether accidentally or intentionally. The individual persons selected to fill these roles shall be above reproach and shall perform their duties carefully, as described in the next section. The duties performed in these roles form the basis of trust in the entire PKI. Two approaches shall be taken to increase the likelihood that these roles may be successfully performed. The first approach is to design and configure the technology to avoid mistakes and prohibit inappropriate behavior. The second is to distribute the functions among several persons, so that any prohibited activity requires collusion. The primary trusted roles defined by this policy are the RA and the CA.

Other trusted roles may be defined in other documents, including those agreements contained in this CP, which describe or impose requirements on the CA's operation.

5.2.1.1	CA	All certificates referencing this policy shall be issued by CA facilities operating under the direct control of a CA. The responsible person or persons identified as operating the CA facilities shall be named and made available during compliance audits. Any CA who has been assigned a policy identifier defined in this document is subject to the stipulations of this policy. A CA's role and the corresponding procedures a CA will follow shall be defined in detail in a certification practices statement (CPS) and, perhaps, also in a concept of operations and procedural handbook (CONOP). A CA's primary responsibilities shall be to ensure that the following functions occur according to the provisions of this policy: certificate generation and revocation; posting certificates and CRLs; performing the daily incremental database backups; administrative functions such as compromise reporting and maintaining the database; hardware cryptomodule programming and management.
5.2.2	Number of persons required per task	A CA shall use commercially reasonable practices to ensure that one person acting alone cannot compromise security. To ensure that one person acting alone cannot compromise security, responsibilities at the CA server shall be shared by multiple roles and persons. Each account on the CA server shall have capabilities limited to and commensurate with the role of the account holder. A CA shall ensure that no single person may gain access to subscriber private keys stored by the CA. At a minimum, procedural or operational procedures shall be in place to perform a key recovery, preferably using a split-knowledge technique, such as two persons each with a separate password, to prevent the disclosure of the encryption key to an unauthorized person. Multi-user control also is required for CA key generation, as outlined in 6.2.3. All other duties associated with CA roles may be performed by an individual person operating alone. A CA shall ensure that any verification process it employs provides for oversight of all activities performed by privileged CA role holders. To ensure the integrity of CA equipment and operation, a separate individual shall be identified for each trusted role. The separation provides a set of checks and balances on the CA operation. Never shall the incumbent of a CA role perform its own auditor function.
5.2.3	Identification and authentication for each role	All CA personnel shall have their identity and authorization verified before they are: included in the access list for the CA site, included in the access list for physical access to the CA system, given a certificate for the performance of their CA roles and given an account on the PKI system. Each of these certificates and accounts (with the exception of CA signing certificates) shall: be directly attributable to a person, not be shared and be restricted to actions authorized for that role through the use of CA software, operating system and procedural controls. CA operations shall be secured using methods such as token-based strong authentication and encryption when the operations are accessed across a shared network.

5.3 Personnel controls

5.3.1	Qualifications of operative personnel	CAs and repositories shall implement and follow personnel and management policies sufficient to ensure the trustworthiness and competence of their employees and of the satisfactory performance of their duties in manner consistent with this policy. These policies shall include the certification of all appropriate personnel as “operative personnel.”

5.3.2	Background check procedures	CAs shall cooperate with and pay for an appropriate background check of their operative personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary) to verify their trustworthiness and competence in accordance with the requirements of this policy and CA's personnel practices, or equivalent. All personnel who fail an initial or periodic background check shall not serve or continue to serve in a trusted role. Background check procedures shall be described in the CPS. They shall be or shall be equivalent to a *category 2* background check, as conducted by the Kansas bureau of investigation, and, if equivalent, as approved by the PMA and the secretary. Before conduct of the background check, the person who is subject of the background shall fully respond in writing to the inquiries on a background disclosure form provided by the PMA or secretary. The PMA or the secretary may request conduct of periodic background checks or update of background checks at their discretion.
5.3.3	Training requirements	A CA shall ensure that all personnel performing duties consistent with the duties of operative personnel for a CA shall receive: comprehensive training in the CA security principles and mechanisms, security awareness, all PKI software versions in use on the CA system, all PKI duties they are expected to perform and disaster recovery and business continuity procedures.
5.3.4	Retraining frequency and requirements	The requirements of 5.3.3 shall be updated periodically to accommodate changes in a CA system. Refresher training shall be conducted as required, and a CA shall review these requirements at least once a year.
5.3.5	Job rotation frequency and sequence	This policy makes no provision regarding frequency or sequence of job rotation. Local policies, which do impose requirements, shall provide for continuity and integrity of the PKI service
5.3.6	Sanctions for unauthorized actions	In the event of actual or suspected unauthorized action by a person performing duties for a CA, the CA shall suspend his or her access to the CA systems.
5.3.7	Contracting personnel requirements	A CA shall ensure that contractor access to the CA site is conducted in accordance with 5.1.1.
5.3.8	Documentation supplied to personnel	Documentation sufficient to define duties and procedures for each role shall be provided to the personnel assigned to that role.

5.4 Security audit procedures

5.4.1	Types of event recorded	CA equipment shall be capable of recording events related to the server (installation, modification, accesses), and the application (requests, responses, actions, publications, and error conditions). Events may be attributable to human action (in any role) or automatically invoked by the equipment. At a minimum, the information recorded shall include the type of event and the time the event occurred. In addition, for some types of events, the success or failure, the source and destination of a message or the disposition of a created object (*e.g.*, a filename) also shall be recorded. When possible, the audit data shall be collected automatically; when this is not possible, a logbook, paper form or other physical medium shall be used. The auditing capabilities of the underlying equipment

		operating system shall be enabled during installation. A record of file manipulation and account management shall be maintained. These events also shall be recorded during normal operation of the CA equipment.
5.4.2	Audit log review	A CA shall ensure that its audit logs are reviewed by CA personnel at least weekly and that all significant events are explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities recorded in the logs. Supporting manual and electronic logs from the CA and RA shall be compared when any action is deemed suspicious. Actions taken following these reviews shall be documented.
5.4.3	Retention period for audit log	The information generated on CA equipment shall be maintained on the CA equipment until the information is moved to an appropriate archive facility. Deletion of the audit log from the CA equipment shall be performed by a person different from the CA operator. This person shall be identified in the CA's CPS. Audit logs shall be retained as archive records in accordance with section 5.5.2.
5.4.4	Protection of audit log	The audit log, to the extent possible, shall not be open for reading or modification by any person or by any automated process other than those that perform audit processing. Any person who does not have modification access to the audit log may archive it. Deletion requires modification access. Weekly audit data shall be moved to a safe, secure storage location separate from the CA equipment.
5.4.5	Audit log backup procedures	Audit logs and audit summaries shall be backed up or copied if in manual form.
5.4.6	Audit collection system, internal vs external	There is no requirement for the audit log collection system to be external to CA equipment. The audit process shall run independently and shall not in any way be controlled by the CA operator. Audit processes shall be invoked at system startup and cease only at system shutdown. Should it become apparent that an automated audit system has failed, the CA operation shall cease until the audit function can be restored. If it is unacceptable to cease CA operation, other procedures, which have been arranged previously with the CA's auditor, shall be employed to provide the audit function.
5.4.7	Notification to event-causing subject	When an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device or application that caused the event.
5.4.8	Vulnerability assessments	Events in the audit process are logged, in part, to monitor system vulnerabilities. The CA shall ensure that a vulnerability assessment is performed, reviewed and revised following an examination of these monitored events.

5.5 Records archival

5.5.1	Types of event recorded	CA archive records shall be sufficiently detailed to establish the proper operation of the CA or the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data shall be recorded for archive for all assurance levels: CA accreditation (if applicable)

certification practice statement
contractual obligations
system and equipment configuration
modifications and updates to system or configuration
certificate requests
revocation requests
subscriber identity authentication data as stated in section 3.1
documentation of receipt and acceptance of certificates
documentation of receipt of tokens
CA re-key
all CRLs issued and/or published
all audit logs
other data or applications to verify archive contents
documentation required by compliance auditors

5.5.2 Retention period for archive

A CA shall maintain documentation of compliance with the provisions of this policy, the Kansas uniform electronic transactions act, article 41 of the Kansas administrative regulations and any related agreements for a period of not fewer than 10 years.

If the original medium cannot retain the archived data for the required retention period, the CA shall transfer the data to a new medium approved by the PMA. Applications required to process the archived data also shall be maintained for the retention period. Before the end of the archive retention period, the CA shall provide the archived data and the applications necessary to read the data to a PMA approved archival facility, which shall retain the applications necessary to read the archived data.

A CA that discontinues providing CA services without making other arrangements for the preservation of the CA's records shall notify the secretary and the subscribers, in writing, of its discontinuance of business, and perform either of the following: (i) revoke all valid certificates and return all records concerning them to the appropriate subscriber; or (ii) submit the records to another CA or authorities as ordered by the secretary.

5.5.3 Protection of archive

No unauthorized user shall be permitted to write to, modify or delete the archive. For the CA, archived records may be moved to another medium when authorized by the PMA. The contents of the archive shall not be released except as determined by the PMA or as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in at least two safe, secure storage facilities separate from the CA.

The CA shall secure its records pursuant to standards that are commercially reasonable within the industry. The records shall be indexed, stored, preserved and reproduced so that they are accurate, complete and accessible to an auditor. They shall be in the English language.

5.5.4 Requirements for time-stamping of records

All records shall be time-stamped.

5.5.5	Procedures to obtain and verify archive information	During any reviews required by this policy, the auditor shall verify the integrity of the archives. Procedures detailing how to create, verify, package, transmit and store the archive information shall be published in the CA's CPS.

5.6 Key changeover

5.6.1	Validity period limitations	A CA uses a private key for creating subscriber certificates; however, relying parties employ the CA certificate containing the CA's public key for the life of the subscriber certificate. Therefore, a CA shall not issue subscriber certificates that extend beyond the expiration dates of the respective CA certificates; in addition, the CA certificate validity period shall extend one user certificate validity period past the last use of the CA private key. To minimize risk from compromise of a CA's private signing key, that key shall be changed more frequently, and only the new key shall be used for certificate signing purposes from that time. The older, but still valid, certificate shall be available to verify old signatures until all of the certificates signed under it also have expired. If the old private key is used to sign CRLs that contain certificates signed with that key, then the old key shall be retained and protected.
5.6.2	Maximum validity period	The following list summarizes the maximum validity period of the CA's signature certificate and the maximum lifetime of the associated authority-signing key (used for certificate signature), separated by a slash. If a CA certificate and key lifetime are selected that are shorter than a subscriber's, then the RA certificate and key lifetime shall be no longer than that of the CA. Note that signature keys that have expired for the purposes of certificate signature still may be used for CRL signature. All values are in years: Levels one and two certificates – 10/5 Levels three and four certificates -- 6/3

5.7 Compromise and disaster recovery

5.7.1	Disaster recovery and business resumption plan	A CA shall establish an appropriate disaster recovery and business resumption plan. The plan shall set up and render operational a facility that is located in a different geographic area and that is capable of providing CA services in accordance with this policy within forty-eight (48) hours of an unanticipated emergency. Such plan shall include a complete and periodic test of readiness for such facility. Such plan shall be detailed in the CPS or other appropriate documentation and shall be readily available to relying parties for inspection.
5.7.2	Secure facility after a natural or other type of disaster	A CA shall establish a disaster recovery plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster, including the compromise of keys or related data. Where a repository is not under the control of the CA, the CA shall ensure that any agreement with the repository provides that a disaster recovery plan shall be established and documented by the repository.
5.7.3	Entity public key is revoked	In the event a CA's certificate must be revoked, the CA immediately shall notify: ITEC, the PMA, the secretary, all CAs to whom it has issued cross-certificates, all of the RAs, all subscribers and all individuals or organizations who are responsible for a certificate used by a device or application. The CA also: shall publish the certificate serial number on an appropriate CRL and revoke all cross-certificates signed with the

revoked digital signature certificate. After addressing the factors that led to revocation, the CA may: generate a new CA signing key pair and re-issue certificates to all entities and ensure that all CRLs and ARLs are signed using the new key. In the event the revocation of any other entity's digital signature certificate is required, *see* section 4.9.

5.7.4 Entity private key is compromised

In the event of the compromise, or suspected compromise, of a CA signing key, the CA immediately shall notify the PMA and all CAs with whom it has cross-certified. In the event of the compromise, or suspected compromise, of any other entity's signing key, an entity shall notify the CA immediately. The CA shall ensure that its CPS or a publicly available document and appropriate agreements contain provisions outlining the procedures it will use to provide notice of compromise or suspected compromise. In the event of the compromise of a CA's digital signature key, the CA shall revoke all certificates issued using that key and provide appropriate notice (see 5.7.3). After addressing the factors that led to key compromise, the CA may: generate a new CA signing key pair; re-issue certificates to all entities and ensure that all CRLs and ARLs are signed using the new key.

5.7.5 Entity public key is downgraded

In the event the downgrade of a CA's certificate is required, a CA immediately shall notify all interested parties including the PMA, other CAs with whom it cross-certified, all RAs and all subscribers.

5.8 CA termination

5.8.1 Procedure upon termination

A CA that discontinues providing CA services without making other arrangements for the preservation of the CA's records shall notify the secretary and the subscribers, in writing, of its discontinuance of business, and perform either of the following: (i) revoke all valid certificates and return all records concerning them to the appropriate subscriber; or (ii) submit the records to another CA or authorities as ordered by the secretary.

5.9 Customer service

5.9.1 Customer service center requirement

A CA shall implement and maintain a customer service center to provide assistance and services to subscribers and relying parties, consistent with this policy. The service shall include a system for receiving, recording, responding to, and reporting problems within its own organization and for reporting such problems to the PMA and the secretary.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pairs for CAs, RAs, repositories and subscribers shall be generated so that the private key only is known by the authorized user of the key pair. Acceptable ways of accomplishing this include having all users (CAs, RAs, repositories and subscribers) generate their own keys on a secure system, not revealing the private keys to anyone else and generating keys in hardware tokens from which the private key cannot be extracted. CA and RA keys shall be generated in hardware

		tokens. Key pairs for repositories and end-entities may be generated in either hardware or software.
6.1.2	Private key delivery to entity	In most cases, a private key will be generated and remain within the crypto boundary of the cryptomodule. If the owner of the module generates the key, then there is no requirement to deliver the private key. If a key is not generated by the subscriber, then the module shall be securely delivered. Accountability for the location and state of the module shall be maintained until delivery of possession. The subscriber formally shall acknowledge receipt of the module. If the subscriber generates the key and the key will be stored by and used by the application that generated it, or if it is delivered on a hardware token in the possession of the subscriber, no further action is required. If the key must be extracted for use by other applications or in other locations, a protected data structure (such as defined in PKCS#12) shall be used. The resulting file may be kept on a magnetic medium or transported electronically.
6.1.3	Public key delivery to certificate issuer	Public keys shall be delivered to a CA in a secure and trustworthy manner, such as a certificate request message. It also may be accomplished by non-electronic means. These means may include, but are not limited to, floppy disk (or other storage medium) sent by registered mail or courier, or by delivery of a token to the CA for local key generation at the point of certificate issuance or request. Off-line methods shall include identity checking and shall not inhibit proof of possession of corresponding private key. Any other methods used for public key delivery shall be detailed in a CPS. In those cases where public/private key pairs are generated by the CA on behalf of the subscriber, the CA shall implement secure procedures to ensure that the token on which the public/private key pair is held is securely sent to the proper subscriber and that the token is not activated prior to receipt by the proper subscriber.
6.1.4	CA public key delivery to users	The public key of a CA's signing key pair may be delivered to subscribers in an on-line transaction in accordance with IETF PKIX part 3, or by another appropriate procedure.
6.1.5	Key sizes	Minimum key length for level four certificates is 1024 bits. Minimum key length for levels three and two shall be between 512 and 1024 bits. Minimum key length for level one certificates is 512.
6.1.6	Public key parameters generation	The digital signature standard shall require key parameters in accordance with FIPS 186. The ECDSA (elliptic curve digital signature algorithm) shall be used in accordance with draft ANSI standard X9.62.
6.1.7	Parameter quality checking	Parameters for the digital signature standard shall be as specified in FIPS186.
6.1.8	Hardware/software key generation	The generation of digital signature keys for all entities shall be generated randomly in a hardware cryptographic module. Any pseudo-random numbers used for key generation material shall be generated by a FIPS approved method.
6.1.9	Key use purposes (as per X.509 v3 key use field)	Keys may be used for authentication, non-repudiation and message integrity. They also may be used for session key establishment. CA signing keys are the only keys that shall be used for signing certificates and CRLs. The certificate key use field shall be used in accordance with PKIX-1 certificate and CRL profile. One of the following key use values must be present in all certificates: digital signature or non-

repudiation. One of the following additional values must be present in CA certificate-signing certificates: Key cert sign or CRL sign. Keys shall be certified for use in signing or encrypting, but not both, unless otherwise provided herein. The use of a specific key is determined by the key use extension in the X.509 certificate. This restriction does not prohibit use of protocols like the secure sockets layer that provide authenticated connections using key management certificates.

6.2 CA private key protection

6.2.1	Private key security	A CA and repository each shall protect its private key(s) in accordance with the provisions of this policy.
6.2.2	Standards for cryptographic module	The applicable standard for cryptomodules shall be FIPS140-1 level 2, unless ITEC, with the assistance of the PMA, determines that other comparable validation, certification, or verification standards shall be sufficient. In such event such standards will be transmitted to CA's by PMA and published by the CA's. Subscribers shall use cryptographic modules, which at a minimum meet the criteria specified in this policy. RAs shall have at least level 2 hardware cryptomodules. A higher level may be used if available or desired. RAs and CAs shall provide the option of using any acceptable cryptomodule, to facilitate the management of certificates. A CA may use hardware or software cryptomodules for CA key generation and protection, validated at level three. Certificates shall be signed using a hardware cryptomodule that meets level three.
6.2.3	Private key multi-person control	Multi-person control requires that more than one person, typically the CA and one or more separate security officers, are independently authorized to the system that will perform CA operations. This procedure shall prevent any single person, CA or otherwise, from gaining access to the CA signing key. Key management and end-entity signature keys may be backed up in multiple tokens without two-person control provided the operations to do so are audited and provided the private keys never exist in an unencrypted form outside the token. CA signing keys shall be backed up only under two-person control. The employees who serve as the two-person control shall be identified in a list that shall be maintained by the CA and made available by the CA for audit.
6.2.4	Private key escrow	A private key never shall be escrowed. For some purposes such as data recovery, however, it will be necessary to provide key escrow and/or key recovery for private keys. The method for this shall be described in the CPS.
6.2.5	Private key backup	An entity optionally may back-up its own private key. If so, the key shall be copied and stored in encrypted form and protected at a level no lower than identified for the primary version of the key.
6.2.6	Private key archival	If a CA is acting as a key recovery agent, it shall archive private key management keys as part of its service. Private keys supporting non-repudiation services never shall be archived. A person optionally may archive his or her own private key.
6.2.7	Private key entry into cryptographic module	Private keys shall be generated and kept inside cryptographic modules evaluated to at least FIPS 140-1 level 3. If a private key is to be transported from one cryptomodule to another, the private key shall be encrypted during transport; private keys never shall exist in plain text form outside the cryptomodule boundary.

6.2.8	Method of activating private key	Private keys shall be activated by activation data stored securely and separately from cryptomodules.
6.2.9	Method of deactivating private key	Cryptomodules that have been activated shall not be left unattended or otherwise open to unauthorized access. After use they must be deactivated, *e.g.* by a manual logout procedure or by a passive timeout. Hardware cryptomodules shall be removed and stored or shall be within the CA's sole control when not in use.
6.2.10	Method of destroying private key	Private keys shall be destroyed when they no longer are needed or when the certificates to which they correspond expire or are revoked. For software cryptomodules, destruction may mean overwriting the data. For hardware tokens, destruction may mean executing an erase command. Physical destruction of hardware is not required.

6.3 Other aspects of key pair management

6.3.1	Retention of verification public keys	A CA shall retain all verification public keys.
6.3.2	Public key archival	Each CA shall protect its private key(s) in accordance with the provisions of this policy.
6.3.2.1	Key replacement	All keys shall have validity periods of no longer than twenty years. Suggested validity period: CA public verification key and certificate - twenty years; CA private signing key - eight years; end-entity public verification key and certificate - twelve years; end-entity private signing key - two years.
6.3.2.2	Restrictions on CA's private key use	The private key used by a CA for issuing certificates shall be used only for signing such certificates and, optionally, CRLs or other validation services responses.
6.3.3	Use periods for the public and private keys	The key use periods for keying material are described in section 6.3.2.1.

6.4 Activation data

6.4.1	Activation data generation and installation	A pass-phrase or PIN (activation data) shall be used to protect access to use of the private key. The activation data may be user selected. If the activation data must be transmitted, it shall be transmitted via a channel of appropriate protection, and distinct in time and place from the associated cryptomodule. If transmission is not accomplished by hand, the user shall be advised of the shipping date, method of shipping, and expected delivery date of any activation data. As part of the delivery method, users will sign and return a delivery receipt. In addition, users also shall receive (and acknowledge) a user advisory statement to help them understand responsibilities in the use and control of the cryptomodule.

6.4.2 Activation data protection

Activation data shall be memorized, not written down. Activation data never shall be shared.

Data used for entity initialization shall be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms. The private keys of entities shall be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms. The level of protection shall be adequate to deter a motivated attacker with substantial resources. If a reusable password scheme is used, the scheme shall include a function to temporarily lock the account after a predetermined number of login attempts.

6.4.3 Other aspects of activation data

This policy makes no provision for the life of activation data; however, it shall be changed periodically to decrease the likelihood that it has been discovered. CAs shall define activation data requirements in their CPSs.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

All CA servers shall include the following functionality, either provided by the operating system or through a combination of operating system, PKI application and physical safeguards:

- access control to CA services and PKI roles;
- enforced separation of duties for PKI roles;
- identification and authentication of PKI roles and associated identities;
- object re-use or separation for CA random access memory;
- use of cryptography for session communication and database security;
- archival of CA and end-entity history and audit data;
- audit of security related events;
- self-test of security related CA services;
- trusted path for identification of PKI roles and associated identities;
- recovery procedures for keys and the CA system.

6.5.2 Computer security rating

A CA's equipment shall meet and be operated to at least a C2 [TCSEC – trusted computer system evaluation criteria] or E2/F-C2 [ITSEC – international trusted system evaluation criteria] rating, or equivalent. A CA's equipment operating at a C2 equivalence shall, as a minimum, implement self-protection, process isolation, discretionary access control, object reuse controls, individual identification and authentication and a protected audit record.

6.6 Life cycle technical controls

6.6.1	Procurement of equipment	Equipment (hardware and software) procured to operate a PKI shall be purchased using a process such as random selection, which will reduce the likelihood that any particular equipment has been subject to tampering. Equipment developed for PKI shall be developed in a controlled environment, and the development process shall be defined and documented. CA equipment shall be packaged securely and delivered using a defined procedure that records the actions of those involved. Tamper-evident packaging shall be used, or equipment shall be hand-carried from a controlled procurement environment to the installation site. The CA equipment shall be dedicated to administering a key management infrastructure. It shall not have installed applications or component software that are not part of the CA configuration. Equipment updates shall be purchased or developed using the same random or like process as the original equipment and shall be installed by trusted and trained personnel in a manner defined in the CPS.
6.6.2	System development controls	A CA shall use CA software that has been designed and developed either under a development methodology such as MIL-STD (military standard)-498, the system security engineering capability maturity model (SSE CMM) or information systems security-engineering handbook. The design and development process shall provide sufficient documentation to easily facilitate third party security evaluation of the CA components and to easily facilitate: third party verification of process compliance; on-going threat risk assessments to influence security safeguard design and minimize residual risk.
6.6.3	Security management controls	A formal configuration management methodology shall be implemented for installation and ongoing maintenance of a CA system. The CA software, when first loaded, shall provide a method for the CA to verify that the software on the system: originated from the software developer; has not been modified prior to installation; and is the version intended for use. The CA shall have adopted and implemented procedures and policies to control and monitor the configuration of the CA system and to verify periodically the integrity of the software. At the time of installation, and at least once every 24 hours, the integrity of the CA system and software shall be validated using these procedures and policies.

6.7 Network security controls

6.7.1	Restrictions on network	CA equipment shall not be connected to more than two network domains at a time. CA equipment that is intended to connect to more than one network classification domain shall have procedures defined in a CPS that prevent information from one domain from reaching another (*e.g.*, equipment shutdown, removable hard drives, switching the network connection). CA equipment may operate through a network guard provided it does not compromise the function of the guard. Protection of CA equipment shall be provided against known network attacks. Use of appropriate boundary controls shall be employed. All unused network ports and services shall be turned off. Only network software necessary to the functioning of the CA application shall be located on the CA equipment. Root CA equipment shall be stand-alone (off-line) configurations.

6.8 Cryptographic module engineering controls

6.8.1	Requirements	Requirements for cryptographic modules are as stated above in section 6.2.2.

7 Certificate and CRL profiles

7.1 Certificate profile

7.1.1	Requirements	Certificates that reference this policy shall contain public keys used for authenticating the sender of an electronic message and verifying the integrity of such messages – *e.g.*, public keys used for digital signature verification. All certificates that reference this policy will be issued in the X.509 version 3 format and may include a reference to the OID for this policy within the appropriate field. The CPS shall identify the certificate extensions supported, and the level of support for those extensions.
7.1.2	Version number and base fields	A CA shall issue X.509 Version 3 certificates, in accordance with the PKIX certificate and CRL Profile. The PKI end-entity software must support all the base (non-extension) X.509 fields:
	Version	version of X.509 certificate, version 3(2)
	Serial number	unique serial number for certificate as well as the certificate extensions defined in section 7.1.3
	Signature	CA signature to authenticate certificate
	Issuer	name of CA
	Validity period	activation and expiration date for certificate
	Subject	subscriber's distinguished name, which may contain additional numbers or letters appended to the common name to ensure the name's uniqueness within the domain of certificates issued by the CA
7.1.3	Certificate extensions	No extension shall modify or undermine the use of X.509 base fields. Additionally:
7.1.3.1	Certificate policies	If the state of Kansas secures an OID, the certificate policies field may be populated in all certificates with one of the policy OIDs and may be set as a non-critical extension.
7.1.3.2	Policy constraints	Reserved.
7.1.3.3	Critical extensions	All entity PKI software shall correctly process critical extensions identified in this policy.
7.1.3.4	Supported extensions	The CPS shall define the use of any extensions supported by a CA, the RAs and end entities.

7.1.4	Name forms	Every DN shall be in the form of an X.501 printable string.
7.1.5	Name constraints	Subject and issuer DNs shall comply with PKIX standards and be present in all certificates.
7.1.6	Certificate policy object identifier	If the state of Kansas secures an OID, each CA shall ensure that the policy OID is contained within the certificates it issues.
7.1.7	Use of key use extension	A CA shall populate and mark as critical the key use extension in a certificate and identify the subscriber's private key as being used either for signing (digital signature and non-repudiation) or for encryption (dataEncipherment and keyEndipherment).
7.1.8	Policy qualifiers syntax and semantics	A CA shall populate the policy qualifiers extension with the URL of its CP.

7.2 CRL profile

7.2.1	Requirements	If used, CRLs shall be issued in the X.509 version 2 format. The CPS shall identify the CRL extensions supported and the level of support for these extensions.
7.2.2	Version numbers	A CA shall issue X.509 version two (2) CRLs in accordance with the PKIX certificate and CRL profile.
7.2.3	CRL and CRL entry extensions	All entity PKI software shall process correctly all CRL extensions identified in the certificate and CRL profile. The CPS shall define the use of any extensions supported by the CA and end entities.

8 Policy administration

8.1 Policy change procedures

8.1.1	Policy review	This policy shall be reviewed by PMA every year. Errors, updates, or suggested changes to this policy shall be communicated to the PMA contact on or before the date ninety days from the anniversary date of the day on which this policy becomes effective. Such communication shall include a description of the change, a change justification and contact information for the person requesting the change. The PMA shall review any notices of errors, updates or suggested changes and provide recommendations to ITEC and CAs. All proposed policy changes shall be disseminated to interested persons (see section 8.2) for a period of thirty days beginning sixty days prior to the anniversary date of the date on which this policy becomes effective (the review period). ITEC shall use its best efforts to accept or reject any proposed changes promptly upon the close of the review period. Notwithstanding, if, in the judgment of ITEC or the PMA, it is determined changes to the policy should be made prior to the annual review, ITEC reserves the right to modify the policy upon notification of the proposed changes to CAs. CAs and RAs shall be given reasonable time to comment, and conform to the proposed changes.

8.1.2	List of items that may change without notification	Notice of all proposed changes to this policy that are considered by the state and a CA, which may materially impact users of this policy (other than editorial or typographical corrections, or changes to the contact details), shall be provided to RAs and shall be posted on the world wide web site of a CA. A CA shall post notice of such proposed changes in its repositories and shall advise subscribers in writing in tangible form or by e-mail of such proposed changes.
8.1.3	List of items subject to notification requirement	All provisions in this policy shall be subject to the notification requirement. Prior to the effective date of any changes to this policy, ITEC through the PMA shall notify all CAs and RAs.
8.1.4	Comment period, process and procedure	Affected users may file comments with the PMA within 30 days of the posting of the original notice. If the proposed change is modified as a result of such comments, a new notice of the modified proposed change shall be given.
8.2	***Publication and notification policies***	
8.2.1	Posting of policy	All CAs shall post a copy of this policy in electronic form on the internet.
8.2.2	Notification procedure	The PMA shall give written notice of any proposed changes to this policy to the secretary, CAs and RAs.
8.2.3	Procedure for comments	Written and signed comments on proposed changes shall be directed to the PMA. Decisions on the proposed changes shall be at the sole discretion of the ITEC with the advice of PMA.
8.2.4	Final change notice	ITEC shall determine the period of time for notice of final change.
8.2.5	Provisions for which change requires a new policy	If the state of Kansas has secured an OID and a policy change is determined by ITEC or the PMA to warrant the issuance of a new policy, the ITEC may require a new object OID for the modified policy.
8.3	***CPS approval procedures***	
8.3.1	Disclosure	When a CA's CPS contains information relevant to the security of the CA, that part of the CPS is not required to be made available publicly. In this instance, the PMA shall prescribe a method for confidential communication of the information it requires, and the CA shall provide it in that method. The information provided in this manner shall not be disclosed by the PMA unless it is determined that it does not qualify as information related to the security of the CA and, therefore, is not exempted under the Kansas open records act.
8.4	***Waivers***	Waivers from this policy shall not be granted for any level of assurance. Variation in a CA's practice either shall be deemed compliant with this policy, or a change shall be requested to this policy.

AGREEMENT between RA and LRA

This agreement is entered into this __ day of _____, 200_ by and between the Information Network of Kansas, registration authority (RA) for the State of Kansas, and _____, (address), a branch or political subdivision of the State of Kansas, local registration authority (LRA).

The parties agree as follows:

1. Subject to the terms and conditions of this agreement, RA agrees to furnish registration authority services for the LRA for the period from _____ through December 31, 200_ at the following price: _____.

2. The parties agree that this agreement is subject to state contract 04294 for digital signature services, the Information Technology Executive Council (ITEC) policy 5200 and its *Policy for the State of Kansas Public Key Infrastructure* (CP) and amendments. *http://da/state/ks/us/itec/*

3. The parties understand and agree that the provisions set out in the DA146a, attached; the CP; and any modifications to this agreement are incorporated and made a part of this contract by reference as though fully set forth herein. The parties agree that these documents are listed in their order of precedence and that these documents are controlling over any other document.

4. The business(es) conducted by LRA to which the services will be dedicated is a lawful business(es).

5. *Limitations on use.* The parties agree that certificates issued under the trusted network are not designed, intended or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems or weapons control systems, where failure could lead directly to death, personal injury or severe environmental damage. RA is not responsible for assessing the appropriateness of the use of a certificate. The parties agree that they will not use or rely upon certificates beyond the limitations set forth in this agreement.

6. The LRA and business partner subscriber have executed an agreement governing the business to be conducted which is attached hereto.

7. The LRA and business partner subscriber have executed the uniform subscriber agreement, which also is attached hereto.

8. RA agrees to process applications for business partner subscriber certificates upon a request from the LRA. The LRA agrees to submit such request in the form approved by the RA. Because of the State of Kansas' interest in the security of the trusted network, the LRA agrees to exercise due diligence in vetting the subscribers in accordance with the CP.

9. LRA agrees that it immediately will report to RA any breach or suspected breach of security concerning services, including any breach upon the part of a subscriber. The latter includes, but is not limited to the following:

a. inaccurate information provided by a subscriber in response to a certificate application;

b. infringement upon the intellectual property rights of any third parties resulting from information provided by a subscriber (including an e-mail address);

c. use by a subscriber of certificate application information or the certificate itself for an unlawful purpose or for any reason not intended and approved by the RA;

d. failure by a subscriber to remain the only person in possession of the private key and the only person with access to the private key;

e. failure by a subscriber to remain the only person in possession of a challenge phrase, PIN, software, or hardware mechanism protecting the private key and the only person with access to the same;

f. use of a subscriber of the certificate as a certificate authority issuing certificates, certification revocation lists or otherwise;

g. use by a subscriber of a private key to create a digital signature when the related certificate is expired, suspended or revoked;

h. attempt by a business partner subscriber to monitor, interfere with or reverse engineer the technical or physical implementation of the trusted network and otherwise intentionally compromise the security of the trusted network.

10. The LRA agrees to and shall adhere to the requirements of the certificate identified above as provided in the Kansas CP.

11. *Payment terms.* RA will invoice LRA for all fees set forth in paragraph paragraph 1, and LRA will pay the fees within thirty (30) days of LRA's receipt of the invoice for such fees. If fees are not paid in accordance with this paragraph, this agreement may be deemed breached and all certificates issued pursuant to it revoked.

12. *Confidentiality.* Any request by either party for treatment of information as confidential shall be resolved by application of the provisions of the Kansas open record act (KORA). KSA 45-215 *et seq.*

13. *Export compliance.* This agreement expressly is made subject to any laws, regulations, orders or other restrictions on the export from the United States of America of software, hardware, or technical information, which may be imposed from time-to time by the government of the United States of America. Regardless of any disclosure made by LRA to RA of an ultimate destination of the software, hardware, or technical information and, notwithstanding anything contained in this agreement to the contrary, LRA will not modify, export, or re-export, either directly or indirectly, any software, hardware, or technical information, or portion thereof, without first obtaining any and all necessary licenses from the United States government or agencies or any other country for which such government or any agency thereof requires an export license or other governmental approval at the time of modification, export, or re-export.

14. *Notices.* All notices, demands, requests, approvals, reports, instructions, consents or other communications which may be required or desired to be given by one party to the other shall be in writing and addressed to the RA or LRA administrators as follows:

RAA	LRAA
_____	_____
_____	_____
_____	_____
e-mail _____	e-mail _____

The RAA or LRAA identified above is the individual authorized to request of the RA issuance or other appropriate action concerning certificates related to this agreement. The RAA and LRAA must be vetted by an independent third party, *e.g.* they may not be vetted by the party employer.

15. The parties agree that they shall retain and maintain for a period of not fewer than five (5) years transaction records related to the services that are subject to this agreement. The records shall be secured pursuant to standards that are commercially reasonable within the industry. They shall be maintained in the form of paper-based documents, retrievable computer-based documents or any form of reproduction approved by the Secretary of State. They shall be indexed, stored, preserved and reproduced so that they are accurate, complete and accessible for audit by the Secretary of State.

16. *Compliance with laws.* Each party agrees that it shall comply with all applicable federal, state and local laws, regulations, ordinances and codes in connection with its performance under this agreement.

17. *Assignment.* The parties agree that any rights under this agreement are not assignable or transferable.

18. *Severability.* If any provision of this agreement, or the application thereof is for any reason and to any extent found to be invalid or unenforceable, the remainder of this agreement (and the application of the invalid or unenforceable provision to other persons or circumstances) shall not be affected by such finding of invalidity or unenforceability, and shall be interpreted in a manner that shall reasonably carry out the intent of the parties.

19. *Force majeure.* Except for payment and indemnity obligations hereunder, neither party shall be deemed in default hereunder, nor shall it hold the other party responsible for, any cessation, interruption or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, act of God, war, armed conflict, terrorist action, labor strike, lockout, boycott, provided that the party relying upon this paragraph (a) shall have given the other party written notice thereof promptly and, in any event, within five (5) days of discovery thereof and (b) shall take all reasonable steps reasonably necessary under the circumstances to mitigate the effects of the force majeure event upon which such notice is based; provided further, that in the event the force majeure event described in this paragraph extends for a period in excess of thirty (30) days in aggregate, the other party immediately may terminate this agreement.

20. Termination. Because of the State of Kansas' interest in the security of the trusted network, if LRA violates any condition of this agreement, this agreement may be deemed breached and all certificates issued pursuant to it revoked.

RA	LRA
By _____	By _____
Title _____	Title _____

AGREEMENT between LRA and Trusted Partner Subscriber

This agreement is entered into this __ day of _____, 200_ by and between _____, (address), a branch or political subdivision of the State of Kansas, local registration authority (LRA), and _____, (address), trusted partner subscriber (subscriber).

The parties agree as follows:

1.The business conducted by LRA and subscriber to which the services will be dedicated is a lawful business.

2. The parties agree that this agreement is subject to state contract 04294 for digital signature services, the Information Technology Executive Council (ITEC) policy 5200 and its *Policy for the State of Kansas Public Key Infrastructure* (CP) and amendments. *http://da.state.ks.us/itec/*

3. To facilitate the issuance of certificates to subscriber, LRA agrees to vet subscriber's credentials and submit them in the proper form to the Kansas registration authority (RA). Subscriber agrees to provide LRA accurate vetting information in accordance with the CP. In order to ensure protection of the Kansas trusted network, the parties agree they will diligently observe the security provisions of the Kansas CP and this agreement.

4. The parties understand and agree that the provisions set out in the DA146a, attached; the CP; and any modifications to this agreement are incorporated and made a part of this contract by reference as though fully set forth herein. The parties agree that these documents are listed in their order of precedence and that these documents are controlling over any other document.

5. *Limitations on use.* The parties agree that certificates issued under the trusted network are not designed, intended or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems or weapons control systems, where failure could lead directly to death, personal injury or severe environmental damage. RA is not responsible for assessing the appropriateness of the use of a certificate. The parties agree that they will not use or rely upon certificates beyond the limitations set forth in this agreement.

6. Subscriber warrants that subscriber and its individual employee subscribers will:

a. provide accurate information in response to a certificate application;
b. not infringe upon the intellectual property rights of any third parties by providing information that would do so (including an e-mail address);
c. not use certificate application information or the certificate itself for an unlawful purpose or for any reason not intended and approved by the RA;
d. remain the only person in possession of the private key and the only person with access to the private key;
e. remain the only person in possession of a challenge phrase, PIN, software, or hardware mechanism protecting the private key and the only person with access to the same;
f. not use the certificate as a certificate authority issuing certificates, certification revocation lists or otherwise;
g. not use a private key to create a digital signature when the related certificate is expired, suspended or revoked;
h. not attempt to monitor, interfere with or reverse engineer the technical or physical implementation of the trusted network and otherwise intentionally compromise the security of the trusted network.

7. Subscriber agrees to immediately report to LRA and RA any breach or suspected breach of security concerning services. The latter include but are not limited to those actions recited in paragraph 6.

8. *Indemnity.* Subscriber agrees to release, indemnify, defend and hold harmless LRA and RA from all liabilities, claims, damages, costs and expenses, including reasonable attorney's fees and expenses relating to or arising out of this agreement or the breach of subscriber warranties, representations and obligations under this agreement.

9. The parties have reviewed the Kansas CP requirements and agree that the following level of certificate is appropriate for the business application subject to this agreement

___ 1
___ 2
___ 3 Currently not available.
___ 4 Currently not available.

10. The parties agree to and shall adhere to the requirements of the certificate identified above as provided in the Kansas CP.

11. *Confidentiality.* Any request by either party for treatment of information as confidential shall be resolved by application of the provisions of the Kansas open record act (KORA). KSA 45-215 *et seq.*

12. *Export compliance.* This agreement expressly is made subject to any laws, regulations, orders or other restrictions on the export from the United States of America of software, hardware, or technical information, which may be imposed from time-to time by the government of the United States of America. Regardless of any disclosure made by subscriber to LRA of an ultimate destination of the software, hardware, or technical information and, notwithstanding anything contained in this agreement to the contrary, subscriber will not modify, export, or re-export, either directly or indirectly, any software, hardware, or technical information, or portion thereof, without first obtaining any and all necessary licenses from the United States government or agencies or any other country for which such government or any agency thereof requires an export license or other governmental approval at the time of modification, export, or re-export.

13. *Notices.* All notices, demands, requests, approvals, reports, instructions, consents or other communications which may be required or desired to be given by one party to the other shall be in writing and addressed to the LRA and subscriber administrators as follows:

LRAA	Subscriber Administrator
_____	_____
_____	_____
_____	_____
e-mail _____	e-mail _____

The LRAA or Subscriber Administrator identified above is the individual authorized to request of the RA issuance or other appropriate action concerning certificates related to this agreement. The LRAA or Subscriber Administrator must be vetted by an independent third party, *e.g.* they may not be vetted by the party employer.

14. The parties agree that each of them shall retain and maintain for a period of not fewer than five (5) years transaction records related to the services that are subject to this agreement. The records shall be secured pursuant to standards that are commercially reasonable within the industry. They shall be maintained in the form of paper-based documents, retrievable computer-based documents or any form of reproduction approved by the Secretary of State. They shall be indexed, stored, preserved and reproduced so that they are accurate, complete and accessible for audit by the Secretary of State.

15. *Compliance with laws.* Each party agrees that it shall comply with all applicable federal, state and local laws, regulations, ordinances and codes in connection with its performance under this agreement.

16. *Assignment.* The parties agree that any rights under this agreement are not assignable or transferable.

17. *Severability.* If any provision of this agreement, or the application thereof is for any reason and to any extent found to be invalid or unenforceable, the remainder of this agreement and the application of the invalid or unenforceable provision to other persons or circumstances shall not be affected by such finding of invalidity or unenforceability, and shall be interpreted in a manner that shall reasonably carry out the intent of the parties.

18. *Force majeure.* Except for payment and indemnity obligations hereunder, neither party shall be deemed in default hereunder, nor shall it hold the other party responsible for, any cessation, interruption or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, act of God, war, armed conflict, terrorist action, labor strike, lockout, boycott, provided that the party relying upon this paragraph (a) shall have given the other party written notice thereof promptly and, in any event, within five (5) days of discovery thereof and (b) shall take all reasonable steps reasonably necessary under the circumstances to mitigate the effects of the force majeure event upon which such notice is based; provided further, that in the event the force majeure event described in this paragraph extends for a period in excess of thirty (30) days in aggregate, the other party immediately may terminate this agreement.

19. *Termination.* Because of the State of Kansas' interest in the security of the trusted network, if subscriber violates any conditions of this agreement, this agreement may be deemed breached all certificates issued pursuant to it revoked.

LRA	Subscriber
By _____	By _____
Title _____	Title _____

STATE OF KANSAS
INDIVIDUAL DIGITAL CERTIFICATE SUBSCRIBER AGREEMENT

Certificate subscribers must read this subscriber agreement before accepting or using a State of Kansas digital certificate.

This subscriber agreement will become effective on the date you accept your State of Kansas digital certificate from the state registration authority (RA).

The State of Kansas digital certificate services are governed by state contract 04294 for digital signature services and the Kansas certificate policy, as amended from time to time, which is incorporated by reference into this subscriber agreement. *See the Information Technology Executive Council (ITEC) policy 5200, "Policy for the State of Kansas Public Key Infrastructure," (CP), http://da.state.ks.us/itec/*

The RA provides limited warranties, disclaims all other warranties, including warranties of merchantability or fitness for a particular purpose, limits liability and excludes all liability for incidental, consequential and punitive damages as stated in the CP.

As a subscriber, you agree to use the certificate and any related registration authority services only in accordance with the CP.

As a subscriber, you demonstrate your knowledge and acceptance of the terms of this subscriber agreement by accepting a digital certificate from the State of Kansas RA and by using the certificate.

As a subscriber, you warrant that you:

a. have provided accurate information in response to a certificate application;
b. upon issuance of a certificate naming the applicant as the subscriber, have reviewed the certificate information to ensure that all subscriber information included in it is accurate and have expressly indicated acceptance or rejection of the digital certificate;
c. have not infringed upon the intellectual property rights of any third parties by providing information that would do so (including an e-mail address);
d. have and will not use certificate application information or the certificate itself for an unlawful purpose or for any reason not intended and approved by the RA;

e. will remain the only person in possession of the private key and the only person with access to the private key;
f. will remain the only person in possession of a challenge phrase, PIN, software, or hardware mechanism protecting the private key and the only person with access to the same;
g. will not use the certificate as a certificate authority issuing certificates, certification revocation lists or otherwise;
h. will not use a private key to create a digital signature when the related certificate is expired, suspended or revoked;
i. will not attempt to monitor, interfere with or reverse engineer the technical or physical implementation of the trusted network and otherwise intentionally compromise the security of the trusted network;
j. will inform the RA within 48 hours of a change to any information included in the certificate or certificate application request; and
k. immediately will report to the RA any breach or suspected breach of security concerning digital certificate services, including but not limited to those listed in this section.

Signed _____